Network Working Group
Request for Comments: 2410
Category: Standards Track

R. Glenn
NIST
S. Kent
BBN Corp

November 1998

Пустой алгоритм шифрования (NULL) и его использование в IPsec

The NULL Encryption Algorithm and Its Use With IPsec

Статус документа

В этом документе содержится проект стандарта Internet для сообщества Internet и запрос на обсуждение в целях развития и совершенствования. Текущее состояние стандартизации и статус протокола можно узнать из документа «Internet Official Protocol Standards» (STD 1). Документ может распространяться без ограничений.

Авторские права

Тезисы

В данном документе определен пустой алгоритм шифрования NULL и его использование с IPsec ESP[1]. Алгоритм NULL никак не меняет полученных для «шифрования» данных. Фактически, NULL, как таковой, просто не делает ничего. NULL обеспечивает для ESP возможность реализации услуг идентификации и контроля целостности без шифрования данных.

Информация о других компонентах, требуемых для реализации ESP, приведена в документах [ESP] и [ROAD].

1. Введение

В этом документе определен алгоритм шифрования NULL и его использование с IPsec ESP [ESP] для обеспечения услуг идентификации и контроля целостности без сохранения конфиденциальности.

NULL является блочным механизмом шифрования, истоки которого теряются в античности. Несмотря на слухи о том, что NSA[2] препятствует публикации этого алгоритма, неочевидно, что это дело их рук. Недавние археологические раскопки показывают, что алгоритм NULL был разработан во времена Римской империи в качестве экспортного варианта шифров Цезаря (Ceaser). Однако, по причине отсутствия 0 в римских цифрах документальные записи алгоритма были утеряны для истории на два тысячелетия.

[ESP] задает использование необязательного алгоритма шифрования для обеспечения конфиденциальности, а также необязательных алгоритмов для идентификации и проверки целостности. Алгоритм шифрования NULL является удобным способом реализации опции «без шифрования». В документе [DOI] такой вариант обозначен, как ESP_NULL.

Спецификация заголовка идентификации IPsec [AH] предоставляет похожий сервис, обеспечиваемый расчетом идентификационных данных, покрывающих поля данных пакета, а также не изменяемые при передаче поля заголовка IP. ESP_NULL не включает заголовок IP в расчет идентификационных данных. Это может быть полезно при организации услуг IPsec через сеть устройств, работающих не по протоколу IP. Обсуждение использования ESP_NULL в отличных от IP сетях выходит за пределы настоящего документа.

В данном документе алгоритм NULL используется в контексте ESP. Дополнительную информацию о совместном использовании компонент ESP для предоставления услуг по защите можно найти в работах [ESP] и [ROAD].

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с RFC 2119 [RFC 2119].

2. Определение алгоритма

Алгоритм NULL математически определяется функцией идентичности (I[3]) применяемой к блоку данных b:

```
NULL(b) = I(b) = b
```

2.1 Ключи

Подобно другим современным шифрам (например, RC5 [RFC-2040]), алгоритм шифрования NULL может использовать ключи различного размера. Однако повышения уровня защиты по мере увеличения длины ключа не происходит.

---

[1]Encapsulating Security Payload — защищенные инкапсулированные данные.
[2]National Security Agency — Агентство национальной безопасности США.
[3]Identity — идентичность.

2.2 Криптографическая синхронизация

Поскольку природа алгоритма NULL не требует поддержки данных о состоянии, ему не требуется предавать IV[1] или иные данные криптографической синхронизации в каждом пакете (или для каждой SA). Алгоритм шифрования NULL объединяет в себе лучшие характеристики блочных и потоковых шифров, не требуя передачи IV или аналогичных данных криптографической синхронизации.

2.3 Заполнение

NULL использует блоки размером 1 байт, позволяющие обойтись без заполнения.

2.4. Производительность

Алгоритм шифрования NULL существенно быстрее других популярных симметричных алгоритмов шифрования, а реализации базового алгоритма доступны для всего оборудования и любой OS[2].

2.5 Тестовые векторы

Ниже приведен набор тестовых векторов для упрощения разработки интероперабельных реализаций алгоритма NULL.

```
test_case =      1
data =           0x123456789abcdef
data_len =       8
NULL_data =      0x123456789abcdef

test_case =      2
data =           "Network Security People Have A Strange Sense Of Humor"[3]
data_len =       53
NULL_data =      "Network Security People Have A Strange Sense Of Humor"
```

3. Операционные требования ESP_NULL

ESP_NULL определяется использованием алгоритма NULL в контексте ESP. В этом параграфе уточняется определение ESP_NULL путем указания требований к рабочим параметрам.

Для механизма обмена ключами IKE[4] [IKE] размер ключа для этого алгоритма **должен** иметь нулевое (0) значение в целях обеспечения интероперабельности и предотвращения всех возможных проблем при экспортном контроле.

Для обеспечения интероперабельности размер IV для данного алгоритма **должен** быть равным 0 битов.

В исходящих пакетах **может** использоваться заполнение в соответствии со спецификацией [ESP].

4. Вопросы безопасности

Алгоритм шифрования NULL не обеспечивает конфиденциальности и не предоставляет никаких других услуг защиты. Он просто является удобным вариантом представления опционального использования шифрования в ESP. В таком случае ESP можно использовать для обеспечения идентификации и контроля целостности без конфиденциальности. В отличие от AH эти средства защиты не применяются ко всем частям заголовка IP. На момент подготовки этого документа не было очевидного понимания, что использование ESP_NULL в чем-либо менее безопасно по сравнению с AH при выборе одного алгоритма идентификации (т. е., пакет, защищенный с помощью ESP_NULL при использовании некого алгоритма идентификации криптографически защищен точно так же, как пакет с использованием AH и того же алгоритма идентификации).

Как указано в [ESP], использование алгоритмов шифрования и идентификации в ESP является необязательным, но для каждой ESP SA должно задаваться использование по крайней мере одного криптографически стойкого алгоритма шифрования или одного криптографически стойкого алгоритма идентификации (или по одному алгоритму каждого типа).

На момент подготовки этого документа не было известно законодательных ограничений на экспорт алгоритма NULL с ключами размером 0 битов.

5. Права интеллектуальной собственности

В соответствии с положениями [RFC-2026] авторы сообщают, что они сообщили о существовании любых прав собственности или интеллектуальной собственности на внесенный и персонально известный каждому автору вклад в работу. Авторы сообщают, что им персонально не известно, что организации, которые они представляют, или третьи лица потенциально владеют правами собственности или интеллектуальной собственности или заявляют такие права.

6. Благодарности

Steve Bellovin предложил и подготовил текст для параграфа о паравах интеллектуальной собственности.

Следует также отметить участников семинара по интероперабельности Cisco/ICSA IPsec & IKE в марте 1998, поскольку документ обязан им своим появлением на свет.

7. Литература

[ESP] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload", RFC 2406[5], November 1998.

[1] Initialization Vector – вектор инициализации. *Прим. перев.*
[2] Операционной системы. *Прим. перев.*
[3] У специалистов по сетевой безопасности специфическое чувство юмора.
[4] Internet Key Exchange – обмен ключами в сети Internet. *Прим. перев.*

[AH] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402[1], November 1998.

[ROAD] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.

[DOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2408, November 1998.

[IKE] Harkins, D., and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC-2026] Bradner, S., "The Internet Standards Process - Revision 3", BCP 9, RFC 2026, October 1996.

[RFC-2040] Baldwin, R., and R. Rivest, "The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms", RFC 2040, October 1996

[RFC-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119[2], March 1997.

6. Адреса редакторов

Rob Glenn

NIST

EMail: rob.glenn@nist.gov

Stephen Kent

BBN Corporation

EMail: kent@bbn.com

С рабочей группой IPsec можно связаться через ее председателей:

Robert Moskowitz

ICSA

EMail: rgm@icsa.net

Ted T'so

Massachusetts Institute of Technology

EMail: tytso@mit.edu

Перевод на русский язык

Николай Малых
nmalykh@gmail.com

7. Полное заявление авторских прав

[5]Документ утратил силу и заменен RFC 4303 и RFC 4305, перевод которых имеется на сайте www.protocols.ru. *Прим. перев.*

[1]Документ утратил силу и заменен RFC 4301, перевод которого имеется на сайте www.protocols.ru. *Прим. перев.*

[2]Перевод этого документа имеется на сайте www.protocols.ru. *Прим. перев.*